DETAILED ACTION

Applicant amends claims 1, 6 & 8 and adds new claims 10-12.

Claims 1, 2, 4-6 and 8-12 are presented for examination.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12July 2010 has been entered.

Response to Arguments

In light of Applicant's Remarks filed 12 July 2010 and the Examiner's Amendment set forth in the instant action, the prior grounds of rejection have been withdrawn.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Pehr Jansson on 28 July 2010.

The application has been amended as follows:

1. (Currently Amended) A method to secure an electronic assembly having a processor and a storage means implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x) ~~and implementing a verification function used to perform an additional calculation on an intermediate result in order to obtain a calculation signature~~, the method comprising:

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;

operating the processor of the electronic assembly according to instructions stored in the storage means to ~~perform the calculation of~~ obtain the result of the elementary operation f(x) by performing a modified calculation in lieu of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is only a one-to-one mapping between a set E and a set E' and h_2 is only an onto mapping of a set F' in a set F, wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional ~~the~~ calculation by the ~~a~~ verification function using the result obtained by the super function in order to obtain the ~~a~~ calculation signature.

6. (Currently Amended) An electronic assembly secured from differential attack and comprising a calculation process processor ~~processing means~~ that includes performing a calculation that includes an elementary operation f(x) of a cryptography algorithm, wherein the electronic assembly comprises storage means for storing instructions to cause the calculation processing means to execute a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature thereby securing the electronic assembly from differential attack; and wherein the calculation process comprises:

operating the calculation processing means of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;

operating the processor of the electronic assembly according to instructions stored in the storage means to obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is only a one-to-one mapping between a set E and a set E' and h_2 is only an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation to obtain the result of

the elementary operation f(x) by the ~~a~~ verification function using the result obtained by the super function in order to obtain the ~~a~~ calculation signature.

8. (Currently Amended) A smart card comprising storage means of a calculation process, processing means of said process, wherein the smart card includes storage means storing instructions implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x) and implementing a verification function used to perform an additional calculation on an intermediate result in order to obtain a calculation signature; and

wherein the calculation process comprises:

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;

operating the processor of the electronic assembly according to instructions stored in the storage means to obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is only a one-to-one mapping between a set E and a set E' and h_2 is only an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and

operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by the ~~a~~ verification function using the result obtained by the super function in order to obtain the ~~a~~ calculation signature.

Allowable Subject Matter

Claims 1, 2, 4-6 and 8-12 are allowed.

The following is an examiner's statement of reasons for allowance:

The prior art, alone or combination, does not teach nor suggest a method to secure an electronic assembly having a processor and a storage means implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x), the method comprising: operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature; operating the processor of the electronic assembly according to instructions stored in the storage means to obtain the result of the elementary operation f(x) by performing a modified calculation in lieu of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is only a one-to-one mapping between a set E and a set E'

and h_2 is only an onto mapping of a set F' in a set F, wherein x is a member of E and f(x) is a member of the set F; and operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature.

The prior art, alone or combination, does not teach nor suggest an electronic assembly secured from differential attack and comprising a calculation process processor that includes performing a calculation that includes an elementary operation f(x) of a cryptography algorithm, wherein the electronic assembly comprises storage means for storing instructions to cause the calculation processing means to execute a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature thereby securing the electronic assembly from differential attack; and wherein the calculation process comprises: operating the calculation processing means of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature; operating the processor of the electronic assembly according to instructions stored in the storage means to obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a super-function operation acting from and/or to a larger set wherein a function f' of a function f is defined as a function f' such that h2(f'(h1(x))) = f(x) wherein h1 is only a one-to-one mapping between a set E and a set E' and h2 is only an onto mapping of a set F' and a set F

wherein x is a member of E and f(x) is a member of the set F; and operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation to obtain the result of the elementary operation f(x) by the verification function using the result obtained by the super function in order to obtain the calculation signature.

The prior art, alone or combination, does not teach nor suggest a smart card comprising storage means of a calculation process, processing means of said process, wherein the smart card includes storage means storing instructions implementing a calculation process that calculates the result of a calculation that includes an elementary operation f(x) of a cryptography algorithm without performing the calculation f(x) thereby avoiding analysis of the operation of the electronic assembly using knowledge of the calculation f(x) and implementing a verification function used to perform an additional calculation on an intermediate result in order to obtain a calculation signature; and wherein the calculation process comprises: operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature; operating the processor of the electronic assembly according to instructions stored in the storage means to obtain the result of the elementary operation f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f' of a function f is defined as a function f' such that $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is only a one-to-one mapping between a set E and a set E'

and h_2 is only an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and operating the processor of the electronic assembly according to instructions stored in the storage means to perform an additional calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure

relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTOL-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435